POLSKIE TOWARZYSTWO
PRAWA ANTYDYSKRYMINACYJNEGO

Profilowanie w kontekście ochrony danych osobowych i zakazu dyskryminacji

Jędrzej Niklas

Profilowanie czyli metoda kategoryzowania osób i przetwarzania informacji wzbudza wiele kontrowersji. Temat ten stał się jedną z kluczowych osi sporu w trakcie trwającej od 2012 roku reformy ochrony danych osobowych na poziomie Unii Europejskiej. W środowisku naukowym oraz organizacji pozarządowych powstają liczne opracowania, które wskazują na wyzwania dotyczące profilowania oraz próby ich regulacji. W poniższej ekspertyzie zamierzam przedstawić najważniejsze problemy, które powstają w wyniku stosowania technik opartych na profilowaniu. Poważnym zagrożeniem, które wiąże się z profilowaniem jest naruszenie prywatności. Jednak jak pisze D. Lyon (opisując techniki nadzoru, jakim niewątpliwe jest również profilowanie): *„Nie należy lekceważyć anonimowości, dyskrecji i prywatności, pamiętajmy jednak, że wiążą się one ściśle z praworządnością i sprawiedliwością, swobodami obywatelskimi i prawami człowieka. Współczesna inwigilacja (...) prowadzi jednak przede wszystkim do segregacji społecznej”* [1]. Ta segregacja i wykluczenie są nierozerwalnie związane z dyskryminacją.

W I. części poniższej ekspertyzy opisuję definicje profilowania, obszary w który znajduje ono zastosowanie (m.in. zapobieganie przestępczości, scoring kredytowy) oraz kluczowe ryzyka z niego wynikające (brak transparentności, dyskryminacja, naruszenie prawa do prywatności). Część II. poświęcona jest regulacjom prawnym dotyczącym profilowania. Przedstawiam tutaj przede wszystkim przepisy dotyczące ochrony danych osobowych oraz ustawodawstwo antydyskryminacyjne. Z kolei w części III. poświęcam uwagę przykładom orzecznictwa dotyczącego profilowania oraz rekomendacjom instytucji międzynarodowych i wspólnotowych. Ostatnia część – IV., zawiera krótkie podsumowanie oraz spis rekomendacji, które mogłyby minimalizować ryzyka dla praw i wolności obywatelskich w związku ze stosowanie profilowania, a zwłaszcza w zakresie ochrony prywatności i wolności od dyskryminacji.

[1] Z. Bauman, D. Lyon, *Płynna inwigilacja. Rozmowy,* Kraków, 2013, s. 26.

Część I
ZAGADNIENIA WPROWADZAJĄCE

1. Definicja profilowania

Na bardzo ogólnym poziomie, profilowanie można porównać do kategoryzowania osób na podstawie na różnych cech. Zarówno tych „niezmiennych" (np. płeć, pochodzenie etniczne, wiek, kolor oczu) jak i „zmiennych" (zachowanie, zwyczaje, preferencje)[2]. Zazwyczaj profile tworzy się za pomocą techniki zwanej „analizą behawioralną". Polega ona na dopasowaniu i korelacji określonego zachowania (np. wyborów konsumenckich) z cechami (np. wiek).

Takie konstruowanie profili można podzielić na trzy etapy. Pierwszym jest zgromadzenie danych anonimowych dotyczących danego zjawiska np. w postaci odpowiedzi na specjalne ankiety dotyczące zakupów. Drugim krokiem jest skorelowanie lub łączenie konkretnych zmiennych, co pozwala przeglądać odpowiedzi z takich ankiet np. z podziałem na płeć. Trzeci etap to z kolei wnioskowanie. Zebrane informacje są analizowane i na ich podstawie tworzy się założenia i modele zachowań. Zostając przy przykładzie wyborów konsumenckich ten ostatni etap może doprowadzić do konkluzji, że np. konkretną markę odzieży najczęściej wybiera grupa kobiet w wieku 18-25 lat[3]. W tym kontekście profilowanie pozwala na „kategoryzowanie osób na podstawie obserwowalnych cech w celu wyciągnięcia wniosków dotyczących innych cech, które nie są obserwowalne"[4].

W literaturze przedmiotu można spotkać bardzo wiele różnych definicji profilowania. Jednak ich wspólnymi cechami jest: wykorzystywanie technik analizy danych, kategoryzacja,

[2] Agencja Praw Podstawowych, *Podniesienie skuteczności działań policji. Rozumienie dyskryminującego profilowania etnicznego i zapobieganie mu: przewodnik*, Luksemburg, 2010, s. 8. http://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_PL.pdf (odcz. z dn. 17.07.2015)
[3] Ibidem, s. 8-9.
[4] Ibidem, s. 9

dedukowania nowych informacja na podstawie tych już znanych, wykorzystywanie nowej wiedzy w określonym celu[5].

Z kolei według Rady Europy profilem jest *„zestaw danych charakteryzujący kategorię osób, który ma zostać zastosowany odniesieniu do danej osoby"* [6]. Samo zaś profilowanie definiowane zostało jako *„automatyczna technika przetwarzania danych polegająca na przypisaniu danej osobie <<profilu>> w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji, zachowań i postaw"*. Na definicji tej opiera się również definicja profilowania przedstawiona w projekcie rozporządzenia ogólnego o ochronie danych osobowych (dalej: RODO)[7] w wersji przyjętej przez Parlament Europejski. Profilowanie w tym dokumencie jest zdefiniowane jako *„każda forma automatycznego przetwarzania danych mająca służyć ocenie niektórych aspektów osobistych tej osoby fizycznej lub też analizie bądź przewidzeniu zwłaszcza wyników w pracy, sytuacji ekonomicznej, miejsca przebywania, zdrowia, preferencji osobistych, wiarygodności lub zachowania tej osoby fizycznej"* (art. 4 pkt 3a).

Profilowanie nie jest jednolitą praktyką, można je podzielić na kilka rodzajów. Jednym z kryteriów jest zakres automatyzacji. W tym kontekście wyróżnia się profilowanie: niezautomatyzowane, zautomatyzowane (gdzie proces analizy i agregacji danych ma charakter automatyczny) i zautonomizowane (gdzie cały proces od analizy, kategoryzacji i ostatecznego wykorzystania profilu jest automatyczny i gdzie nie ma udziału człowieka)[8]. Inny podział związany jest z zakresem osób branych pod uwagę przy profilowaniu. Mamy więc tworzenie profili grupowych, przy którym gromadzi się informacje o wielu osobach. Ma to umożliwić na statystyczne wnioskowanie o wystąpieniu danej cechy, na podstawie

---

[5] V. Ferraris, F. Bosco, G. Cafiero, E. D'Angelo, Y. Suloyeva, *Defining Profiling. Working paper, 2014*, s. 3. http://www.unicri.it/special_topics/citizen_profiling/WP1_final_version_9_gennaio.pdf (odcz. z dn. 17.07.2015)

[6] Rekomendacja Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profilii, CM/Rec (2010) 13, polskie tłumaczenie http://www.giodo.gov.pl/plik/id_p/2155/j/pl/. (odcz. z dn. 17.07.2015)

[7] Projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) COM (2012) 11, wersja przyjęta przez Parlament Europejski http://www.europarl.europa.eu/sides/getDoc.do;jsessionid=03B470D165FDB86CDD64F05ED80EEB99.node2?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//pl (odcz. z dn. 17.07.2015)

[8] M. Hildebrandt, *Defining profiling: new type of knowledge?*, [w:] M. Hildebrandt, S. Gutwirth, *Profiling the European Citizens, Cross-Disciplinary Perspectives*, Springer, 2008, s. 28-30.

przynależności tej osoby do populacji. Z kolei profilowanie indywidualne polega na tym, że gromadzi się dane dotyczące jednej osoby z różnych źródeł (data mining)[9]. Muszą tutaj istnieć silne podstawy by sądzić, że dane dotyczą jednej i tej samej osoby, a na ich podstawie, można wytworzyć pewną nową informację. Grupa Robocza art. 29[10] wskazuje również na podział dotyczący metod pozyskiwania danych na potrzeby profilowania. Stosując taki podział, istnieje profilowanie predykcyjne – *„tworzone w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w czasie, w szczególności poprzez monitorowanie odwiedzanych stron”*. Innym rodzajem jest profilowanie jawne, gdy profile *„tworzy się na podstawie danych osobowych przekazywanych w ramach usługi sieciowej przez same osoby, których dane dotyczą np. podczas rejestracji”*[11].

2. Obszary zastosowania profilowania

Profilowanie jest metodą wykorzystywaną w różnych obszarach i kontekstach. Jednym z nich jest zapobieganie i zwalczanie przestępczości, w tym terroryzmu. Przykładem takiego zastosowania jest np. analizowanie danych pasażerów linii lotniczych – danych PNR (patrz część II. pkt 3 ppkt a). Wykorzystywanie informacji o tym skąd, gdzie, jak często, z kim dana osoba podróżuje ma umożliwić organom ścigania „wyłapanie” potencjalnych terrorystów czy osób handlujących żywym towarem. Jak w każdym rodzaju profilowania ustala się tutaj pewne zachowania czy cechy, które mogą charakteryzować podejrzanego. Z kolei Wielkiej Brytanii działa tzw. system E-CAF[12]. Gromadzi on dane z baz policyjnych, opieki społecznej i szkół. Analiza tych informacji ma identyfikować dzieci, które mają lub mogą mieć problemy z wymiarem sprawiedliwości oraz umożliwić interwencję odpowiednich organów państwowych. We Włoszech funkcjonuje natomiast mechanizm *Redditometro*, który

[9] V. Ferraris, *op. cit., 5-6.*
[10] Grupa Robocza art. 29 jest niezależnym organem doradczym w zakresie ochrony danych i prywatności; powstała na podstawie unijnej dyrektywy o ochronie danych osobowych z 1995 roku. Grupa skupia przedstawicieli organów ochrony danych osobowych z państw członkowskich i przedstawicieli instytucji unijnych.
[11] Uwagi Generalnego Inspektora Ochrony Danych Osobowych w sprawie ustawy o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw, DOLiS - 033 - 70/13/MK/51620, s. 7.
[12] R. van Brakel, P. De Hert, *Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies*, CPS, nr 20, 2011, s. 174.
http://www.vub.ac.be/LSTS/pub/Dehert/378.pdf (odcz. z dn. 17.07.2015)

umożliwia śledzenie nadużyć podatkowych[13]. System gromadzi dane wynikające z deklaracji podatkowych oraz informacje pochodzące z banków i innych instytucji finansowych. System analizuje te informacje automatycznie i wskazuje na podejrzane transakcje, które mogą prowadzić do naruszenia przepisów podatkowych.

Profilowanie jest metodą bardzo często stosowaną w marketingu. Jego zasadniczym celem jest najczęściej dopasowanie odpowiedniej reklamy czy produktu do osoby. Istotnym elementem tego procesu, jest analizowanie danych o klientach, która prowadząc do pewnej generalizacji ma umożliwić przewidywanie ich zachowań. Profilowanie takie odbywa się w ramach np. programów lojalnościowych. Zyskiem dla firmy – oprócz wiernego klienta – są również jego dane[14]. Badania dotyczące niemieckich programów lojalnościowych wykazały, że w ich trakcie zbierane są takie informacje jak np. data narodzin, płeć, stan cywilny konsumentów. Dane są później łączone z informacjami o wybranych przez nich produktach czy usługach. Dane wykorzystywane są do badań, tworzenia strategii marketingowych oraz dostarczenia zindywidualizowanej reklamy[15]. Podobny mechanizm ma profilowanie w Internecie. Specjalne algorytmy analizują dane dotyczące zachowań czy historii przeglądanych stron użytkowników. Wykorzystywane są do tego głównie pliki cookies. Na tej podstawie można stworzyć profil użytkownika i dopasować dla niego „potencjalnie" interesującą reklamę czy rekomendować konkretny produkt. Coraz większe znaczenie ma analizowanie informacji pochodzących z portali społecznościowych. W tym przypadku w grę wchodzą nie tylko informacje o przeglądanych stronach, ale wszelkie dane dotyczące konkretnej osoby, jej powiązaniach, miejscu zamieszkania, znajomych itp.

Innym przykładem tworzenia profili jest tzw. scoring kredytowy[16]. Jest to metoda oceny wiarygodności osoby ubiegającej się o pożyczkę. Wynik scoringu jest przedstawiany w formie punktowej. Wyższa liczba punktów oznacza większe prawdopodobieństwo terminowej spłaty kredytu. Banki stosując scoring tworzą pewien model klienta, który będzie

[13] K.Ball, K.Spiller (red.), *Increasing Resilience in Surveillance Societies. Surveillance Impact Report*, 2014 s. 426-430. http://irissproject.eu/wp-content/uploads/2014/06/D3.2-Surveillance-Impact-report1.pdf1.pdf (odcz. z dn. 17.07.2015)

[14] V. Ferraris, *op. cit.*, 28.

[15] M. Kamp, B. Körffer, M. Meints, *Profiling of customers and consumers – customer loyalty programmes and scoring practices*, [w:] M. Hildebrandt, S. Gutwirth, *Profiling the European Citizens, Cross-Disciplinary Perspectives*, Springer, 2008, s. 219-235.

[16] Zob. Biuro Informacji Kredytowej, Ocena Punktowa, https://www.bik.pl/ocena-punktowa (odcz. z dn. 17.07.2015).

wzorem oceny dla innych. Nie jest do końca jasny zakres danych branych przy analizie scoringowej. Zazwyczaj też algorytmy wykorzystywane przy scoringu podlegają ochronie własności intelektualnej. Na podstawie dostępnych źródeł można wnioskować, że przy scoringu brane są pod uwagę np.: wiek, historia kredytowa, miejsce zamieszkania, zawód, stan cywilny[17].

Metody oparte na profilowaniu zaczynają być również wdrażane w takich obszarach jak ochrona zdrowia czy polityka społeczna. Placówki ochrony zdrowia generują ogromne ilości danych o pacjentach i udzielanych świadczeniach. Już teraz informacje te są analizowane i dostosowywane do oceny efektywności określonego leczenia, zarządzania placówką czy wykrywania nadużyć finansowych. Profilowanie jest też stosowane w instytucjach realizujących politykę społeczną. Jednym z takich przykładów są polskie urzędy pracy, które od 2014 roku dokonują profilowania osób bezrobotnych, oceniając ich „potencjał zatrudnienia" (więcej patrz część II pkt. 3 ppkt. b). Profilowanie warunkuje dostęp do konkretnych form wsparcia, ma pomóc w lepszym zarządzaniu małymi środkami finansowymi i zwiększyć efektywność samych urzędów pracy.

3. Kluczowe problemy dotyczące profilowania

a. Błędy i transparentność

Z profilowaniem wiąże się wiele problemów. Szczególne ryzyka powstają gdy z analizy danych statystycznych wnioskuje się o występowaniu nieznanej dotąd cechy u konkretnej osoby. Metoda taka bazująca na korelacjach i jest obarczona dużym prawdopodobieństwem występowania błędów. Ryzyko to nasila się gdy na podstawie profilowania podejmuje się automatycznie decyzje. Rola człowieka w tym procesie zaczyna być minimalizowana, a odpowiedzialność spoczywać na „mitycznym komputerze". Jak słusznie zauważyła przewodnicząca amerykańskiej Federalnej Komisji Handlu, Edith Ramirez: *„Jednostki mogą być ocenianie nie ze względu na to co zrobiły lub co zrobią w przyszłości, ale również na podstawie wniosków wynikających z korelacji wyciągniętych przez algorytmy, które sugerują,*

[17] K. Ball, *op. cit.*, s. 78-135.

że taka osoba może być złym kredytobiorcą czy klientem ubezpieczalni, nieodpowiednim kandydatem do zatrudnienia lub przyjęcia do szkoły"[18].

Co więcej profilowanie zazwyczaj jest metodą opartą na pewnych wzorach matematycznych, które nie uwzględniają wszystkich skomplikowanych sytuacji życiowy. Przykładem jest np. profilowanie pomocy dla osób bezrobotnych – gdzie grupę przyczyny, dla których osoba pozostaje bez pracy ograniczono do 22 przypadków, które nie pokrywają się ze wszystkimi ludzkimi problemami.

Bardzo często algorytmy wykorzystywane w trakcie profilowania, jak w przypadku scoringu kredytowego, objęte są tajemnicą handlową. Obywatele i konsumencie nie mają więc pełnego wglądu do zakresu przetwarzanych w trakcie profilowania danych. O ile uprawnienia wynikające z przepisów dotyczących ochrony danych osobowych, pozwalają na zapoznanie się z rodzajem wykorzystywanych informacji, o tyle możliwość zapoznania się z samą logiką przetwarzania (to w jaki sposób dana informacja jest punktowana, jak wpływa na ostateczny wynik) nie jest już tak oczywista. Brak takich gwarancji może być szczególnie trudny do zaakceptowania, w przypadku korzystania z metod opartych na profilowaniu przy zapobieganiu i zwalczaniu przestępstw. W tych przypadkach *„osoby nie mają możliwość by zakwestionować ani faktów ani metody ich analizowaniu, które wpływają na osiągnięty efekt"*[19].

b. Dyskryminacja

Profilowanie może również prowadzić do dyskryminacji, zarówno tej bezpośredniej jaki i pośredniej[20]. Pojawia się ono przede wszystkim wtedy gdy w trakcie profilowania uwzględnia się takie cechy jak: płeć, wiek, pochodzenie etnicznie, stan zdrowia, orientacja seksualna itp.

---

[18] Przemówienie Edith Ramirez https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf (odcz. z dn. 17.07.2015).

[19] D. J. Steinbock, *Data Matching, Data Mining and due process*, Georgia Law Review, vol. 40, nr 1, s. 7-8.

[20] Przyjmuje tutaj definicje ujęte w tzw. ustawie antydyskryminacyjnej gdzie dyskryminacja bezpośrednia oznacza: „sytuację, w której osoba fizyczna ze względu na płeć, rasę, pochodzenie etniczne, narodowość, religię, wyznanie, światopogląd, niepełnosprawność, wiek lub orientację seksualną jest traktowana mniej korzystnie niż jest, była lub byłaby traktowana inna osoba w porównywalnej sytuacji"; a dyskryminacja pośrednia „sytuację, w której dla osoby fizycznej ze względu na płeć, rasę, pochodzenie etniczne, narodowość, religię, wyznanie, światopogląd, niepełnosprawność, wiek lub orientację seksualną na skutek pozornie neutralnego postanowienia, zastosowanego kryterium lub podjętego działania występują lub mogłyby wystąpić niekorzystne dysproporcje lub szczególnie niekorzystna dla niej sytuacja, chyba że postanowienie, kryterium lub działanie jest obiektywnie uzasadnione ze względu na zgodny z prawem cel, który ma być osiągnięty, a środki służące osiągnięciu tego celu są właściwe i konieczne"

Gdy informacje takie są wykorzystywane w algorytmie, na podstawie którego podejmuje się określone decyzje np. odmowa kredytu czy wyższa cena za bilet samolotowy, może dochodzić do dyskryminacji (dyskryminacja bezpośrednia). Np. badania przeprowadzane na Uniwersytecie Carnegie Mellon wskazały, że algorytmy stosowane przez Google prowadzą do tego, że kobietom wyświetlane są oferty prac dużo gorzej płatnych niż mężczyznom[21]. Algorytmy jednak mogą również brać pod uwagę takie dane, które na pierwszy rzut oka nie są kontrowersyjne jak np. miejsce zamieszkania. Bywa jednak, że taka cecha może prowadzić do dyskryminacji, gdy określone miejsce jest zamieszkane np. przez mniejszość etniczną. Przykładem takiej sytuacji była sprawa jednej z największych amerykańskich firm ubezpieczeniowych Allstate. Korporacji zarzucano, że przy tworzeniu i stosowaniu scoringu, wykorzystuje informacje, które mogą prowadzić do dyskryminacji osób pochodzących z mniejszości Afro-Amerykańskiej i latynoskiej. Stosowanym przy tym był fakt zamieszkiwania w określonej okolicy. Te miejsca, w których mieszkali przedstawiciele mniejszości, były gorzej oceniane. W efekcie osoby pochodzące tych mniejszości automatycznie otrzymywały oferty droższych polis ubezpieczeniowych [22] . Problem dyskrymiacnji dostrzega się również w przypadku profilowania, z którego korzysta się przy zwalczaniu i zapobieganiu przestępczości. W debacie publicznej od bardzo dawna porusza się temat tzw. profilowanie etnicznego i rasowego – czyli podejmowania pewnych czynności (np. zatrzymania) przez organy ścigania wobec konkretnych osób, tylko ze względu na ich przynależność do konkretnej grupy etnicznej. Przykładem tego jest np. sprawa Ramiego Faresa – Polaka palestyńskiego pochodzenia, któremu odmówiono przyznania akredytacji na Euro 2012[23]. Fares chciał zostać wolontariuszem podczas imprezy, warunkiem było jednak otrzymanie opinii, w której policja (na wniosek UEFA) stwierdza, że kandydat nie „stwarza zagrożenia dla bezpieczeństwa turnieju". W przypadku Faresa opinia była negatywna, co okazało się równoznaczne z odmową akredytacji UEFA, niezbędnej do wejścia na stadion. Wszystko wskazywało na to, że jedynym powodem tej decyzji było pochodzenie kandydata

[21] A. Datta, M. C. Tschantz, A. Datta, *Automated Experiments on Ad Privacy Settings, A Tale of Opacity, Choice, and Discrimination*, Proceedings on Privacy Enhancing Technologies, 2015.
[22] Sprawa Dehoyos v. Allstate http://caselaw.findlaw.com/us-5th-circuit/1292810.html (odcz. z dn. 17.07.2015)
[23] Por. Gazeta Wyborccza, Policja dyskryminuje ciemnoskórych?, http://m.wyborcza.pl/wyborcza/1,105226,11810594,Policja_dyskryminuje_ciemnoskorych_.html (odcz. z dn. 17.07.2015)

na wolontariusza. Innym przykładem są systemy analizujące dane PNR (dane dotyczące pasażerów linii lotniczych). W 2009 roku w Wielkiej Brytanii ujawniono saklę wykorzystywania tych informacji. Jak się okazało, brytyjska policja w samym 2009 roku miała swobodny dostęp do danych ponad 47 tys. pasażerów. Na ich podstawie opracowano 14 tys. raportów na temat potencjalnie podejrzanych osób. Szczególnie podejrzanymi byli pasażerowie lecący na Bliski Wschód, do Pakistanu, Afganistanu czy Iraku[24].

c. Prawo do prywatności

Wiele zagrożeń związanych z profilowaniem wiąże się również z ochroną prywatności i autonomii informacyjnej. W przypadku profilowania bardzo często człowiek zostaje zredukowany do przedmiotu określonej operacji na danych, którą przeprowadza komputer. Jednostka może tracić kontrolę nad informacjami, które jej dotyczą. Ryzyko pojawia się zwłaszcza wtedy gdy osoba nie wie, że jest profilowana lub nie posiada wystarczających informacji np. o tym jakie dane są wykorzystywane przy operacji lub skąd pochodzą. Istnieje tutaj silny związek z możliwością podejmowania decyzji o własnym życiu, a w konsekwencji samostanowienia – *„brak informacji o tym w jaki sposób zostałam skategoryzowana oraz jakie wynikają z tego konsekwencje prowadzi do przeobrażenia zasady samostanowienia w kpinę”* (hidebrat 2009, 243).

Profilowanie może prowadzić do naruszenia prywatności nie tylko gdy tworzy się indywidualny profil, ale również kwalifikuje osobę do określonej grupy. Z perspektywy autonomii informacyjnej istotne jest to, że profilujący wie, że osoba należy do określonej kategorii (np. osób homoseksualnych, osób z nadwagą) i jest w stanie tę wiedzę wykorzystać. Obecnie istnieją ku temu możliwości techniczne. Niedawne badania przeprowadzone na Uniwersytecie w Cambridge, wykazały, że analiza danych umieszczanych na Facebooku

[24] J. Lewis, *Outrage at secret probe into 47,000 innocent flyers*, Daily Mail, 2010, http://www.dailymail.co.uk/news/article-1278782/Outrage-secret-probe-47-000-innocent-flyers.html (odcz. z dn. 17.07.2015)

pozwala wykazać, w znaczącej większości przypadków orientację seksualną danej osoby, pomimo, że ona tej informacji nie ujawnia[25].

Część II
ZAGADNIENIA PRAWNE

1. Prawo do prywatności i ochrony danych osobowych

Profilowanie jako pewna operacja na danych podlega przepisom dotyczącym ochronie danych osobowych. Z kolei przetwarzanie, gromadzenie i udostępnianie danych o obywatelach stanowi ograniczenie prawa do prywatności oraz autonomii informacyjnej. Art. 47 Konstytucji RP formułuje prawo do *„ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu prywatnym”* (zbiorczo określne mianem prawem do prywatności). Art. 51 ust 2 zakazuje władzy publicznej pozyskiwania, gromadzenia i udostępniania *„innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawa”*. Prawo do prywatności oraz ochrona autonomii informacyjnej nie mają charakteru absolutnego. Wszelkie ograniczenia ww. praw muszą spełniać wymogi stawiane przez art. 31 ust 3. Konstytucji RP i realizować przesłankę niezbędności gromadzenia informacji o obywatelach w demokratycznym państwie prawnym z art. 51 ust. 2 Konstytucji RP.

Kluczowym aktem prawnym dotyczącym przetwarzania danych osobowych jest w polskim systemie prawnym ustawa o ochronie danych osobowych z 1997 roku[26] (dalej: u.o.d.o). Ustanawia ona podstawowe pojęcie definicje, wskazuje na zasady przetwarzania danych, konstytuuje uprawnienia podmiotu danych, obowiązki administratora itp. Zgodnie z tym aktem prawnym za dane osobowe należy uznać *„wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej”* poza sytuacjami, gdy do określenia tożsamości danej wymagane są działania związane z nadmiernymi kosztami, pracą

[25] M.Kosinski, D. Stillwell, T. Graepel, Private traits and attributes are predictable from digital records of human behawior, PNAS Early Edition, 2013, http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf, (odcz. z dn. 17.07.2015)
[26] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U.2002.101.926 ze zm.

lub czasem (art. 6 ust 1 i 3). Ustawa o ochronie danych osobowych implementowała do polskiego systemu prawnego postanowienia Dyrektywy 95/46/WE[27].

a. Podstawowe uprawnienia podmiotu danych

Jak wskazuje rozdział 4 u.o.d.o osoba, której przetwarzane dane dotyczą (czyli podmiot danych) posiada określone uprawnienia. Wśród nich można wyróżnić te o charakterze: informacyjnym, korekcyjnym i zakazowym[28]. Podmiot danych ma więc prawo do uzyskania wyczerpujących informacji o tym czy istnieje zbiór w którym jego/jej dane są przetwarzane, kto przetwarza, zakresie i sposobie przetwarzania danych, źródle pochodzenia danych czy o tym komu dane są udostępniane (art. 32 ust.1 pkt. 1-5). Każdy jest również uprawniony do uzupełnienia, uaktualnienie, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia jeżeli są one niekompletne, nieaktualne lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane (art. 32 ust.1 pkt. 6). Z kolei uprawnienia o charakterze zakazowym dotyczą prawa wniesienia sprzeciwu wobec przetwarzania danych osobowych w celach marketingowych albo w sytuacjach szczególnych oraz wobec przekazywania danych innemu administratorowi (art. 32 ust.1 pkt. 8-9). Z każdym z powyższych uprawnień związany jest również odpowiedni obowiązek administratora danych, który jest wskazywany bezpośredni w ustawie. W razie niewypełnienia przez administratora obowiązków, podmiotowi przysługuje uprawnienie do wnioskiem do GIODO o nakazanie dopełnienia obowiązku.

b. Wolność od automatycznego podejmowania decyzji

Istotne znaczenie w kontekście profilowania ma art. 26a u.o.d.o., który wskazuje na generalny zakaz podejmowania ostatecznych rozstrzygnięć w indywidualnej sprawie, na podstawie danych osobowych, jeżeli treść takiego rozstrzygnięcia jest wyłącznie wynikiem operacji na tych danych, prowadzonych w systemie informatycznym. Stanowi on implementację art. 15 dyrektywy 95/46. Przepis ten jest dosyć nietypowy w kontekście samej u.o.d.o., ponieważ

[27] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U.UE.L.1995.281.31 ze zm.
[28] J. Barta, P, Fajgelski, R. Markiewicz, *Ochrona danych osobowych. Komentarz,* Warszawa, 2011, s. 583.

reguluje nie tylko sam proces przetwarzania danych, ale również wskazuje na jego konsekwencje. *„Można twierdzić, iż u podstaw regulacji wyrażonej w art. 26a, leży myśl, że wydawanie rozstrzygnięć zawierających ocenę osoby i przez to dotykających jej spraw osobistych nie powinno być przekazywane komputerowi, za tego rodzaju decyzje powinien być zawsze odpowiedzialny człowiek”*[29]. Człowiek jako jednostka posiadająca pewien zakres „autonomii informacyjnej”, nie może być degradowany jedynie do „obiektu komputerowej operacji”. Zakaz ujęty w art. 26a obejmuje rozstrzygnięcia ostateczne i które wynikają z operacji na danych. Rozstrzygnięcie nie musi mieć formy decyzji administracyjnej. Według przedstawicieli doktryny, użyte w przepisie słowo „ostateczny” wskazuje jednak, że od rozstrzygnięcia takiego nie można się odwołać i nie może ono mieć również charakteru wstępnego, który podlega zatwierdzeniu przez człowieka[30]. Argument ten jednak nie jest w pełni przekonywujący. Wydaje mi się, że przy stosowaniu tego przepisu bardzo wiele zależy od kontekstu. Z zastosowaniem art. 26a można mieć do czynienia gdy pomimo, że system informatyczny warunkuje zatwierdzenie decyzji przez człowieka, to czynność ta jest wykonywana niejako automatycznie, bez analizowania sytuacji osoby i bez większego zaangażowania ze strony podmiotu podejmującego rozstrzygnięcie. O „ostateczność rozstrzygnięcia” nie powinny tylko wynikać z przesłanek formalnych ale również faktycznych. Równie istotne jest, że rozstrzygnięcie o którym mowa musi być podejmowane wyłącznie na podstawie operacji na danych prowadzonej w systemie informatycznym – jednym słowem musi mieć ono automatyczny charakter.

Wolność od rozstrzygnięć o których mowa w art. 26a przysługuje gdy spełnione są kumulatywnie cztery warunki: a) Zostaje podjęte rozstrzygnięcie, b) rozstrzygnięcie jest podejmowane w indywidualnej sprawie, c) decyzja jest konsekwencją pewnej oceny cech danej jednostki, d) rozstrzygnięcie jest wynikiem automatycznego procesu prowadzonego w systemie informatycznym[31].

W związku z generalnym zakazem podejmowania takich rozstrzygnięć wiążą się również określone uprawnienia podmiotu danych. Przede wszystkim osoby mają prawo do uzyskania informacji o przesłankach podjęcia ostatecznego rozstrzygnięcia indywidualnej sprawy (art.

[29] Ibidem, s 543.
[30] Ibidem, s. 545.
[31] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa, 2010, s. 147.

32 ust.1 pkt. 5a u.o.d.o). To ważne uprawnienie ma pozwolić na zapoznanie się z *„logicznym układem i strukturą automatycznego przetwarzania danych”*[32]. Uprawnienie to niestety może być ograniczone m.in. ze względu na ochronę tajemnicy handlowej w zakresie wykorzystywanego algorytmu. Innym uprawnieniem jest upoważnienie do wystąpienia z żądaniem ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem art. 26 ust. 1 u.o.d.o. Ponowne rozpatrzenie sprawy oznacza, że podjęte rozstrzygnięcie nie będzie tylko wyłącznie wynikiem operacji na danych prowadzonych przez system informatyczny. Należy dodać, że ponowne rozstrzygnięcie nie musi być korzystne dla żądającego. Przedmiotem tej szczególnej ochrony jest *„wyłącznie eliminacja określonego trybu podejmowania rozstrzygnięć”*[33]. W przypadku gdy administrator danych nie uwzględni żądania, sprawa w raz z uzasadnieniem jest przekazywana do GIODO. Organ ten może wówczas wydać decyzję niestwierdzającą naruszenia art. 26a ust.1 lub nakazującą przywrócenie stanu zgodnego z prawem, np. ponownego rozpatrzenia sprawy. Generalny zakaz wynikający z art. 26a ust. 1 nie ma zastosowania w sytuacji gdy automatyczne podejmowanie decyzji zostało jest związane z zawarciem lub wykonywaniem umowy i uwzględnia wniosek podmiotu danych albo zezwalają na to przepisy prawa, które przewidują również środki ochrony uzasadnionych interesów osoby, której dane dotyczą.

Art. 15 dyrektywy 95/46 który dotyczy automatycznego podejmowania decyzji, różni się w pewnym zakresie od art. 26a u.o.d.o. Nie przedstawiając szczegółowo tych różnic należy tylko zasygnalizować, że dyrektywa reguluje kwestie dotyczące tego sposób podejmowania decyzji, jeżeli wywołuje ona skutki prawne lub mają na istotny wpływ na osobę której dotyczą. Dyrektywa ustanawia też wyjątki od tego generalnego zakazuj, które mogą wynikać z konkretnego przepisu prawnego lub zawierania umowy. Wyjątkom tym muszą jednak towarzyszyć odpowiednie środki, które zabezpieczaną interesy podmiotu danych. Dyrektywa wskazuje na przykłady takich gwarancji jak: uwzględnienie wniosku zainteresowanej osoby przy podejmowaniu decyzji albo przedstawienie swojego punktu widzenia. Gwarancje te mają zapewnić, że podmiot danych będzie współuczestniczył w podejmowaniu decyzji, minimalny udział sprowadza się tutaj do „prawa do bycia wysłuchanym”[34]. Art. 15

[32] J. Barta, *op. cit.*, s. 597.
[33] Ibidem, s. 606.
[34] M. Jagielski, *op. cit.*, s. 151.

dyrektywy 95/46/WE został różnie implementowany w konkretnych państwach członkowskich UE. W kontekście proponowanych gwarancji dla podmiotu danych warto jednak przytoczyć niektóre przykłady, gdzie podmiot danych zyskuje szersze uprawnienie. Greckie rozwiązania obejmują nie tylko prawo do przedstawienia swojego zdania w przypadku decyzji podjętej na podstawie automatycznego przetwarzania danych, ale również uprawnienie by zwrócić się do sądu o natychmiastowe zawieszenie lub stwierdzenie nieważności takiej decyzji. Z kolei w Hiszpanii podmiot danych ma prawo do uzyskania szczegółowych informacji związanych z decyzją opartą na przetwarzaniu danych czyli „kryteriów oceny" oraz „oprogramowaniu użytym do tej oceny". Brytyjskie ustawodawstwo określa natomiast, że każdy ma prawo do zwrócenia się do jakiegokolwiek administratora z żądaniem informacji o tym czy wobec niego została podjęta decyzja oparta na automatycznym przetwarzaniu danych. Jeżeli decyzja taka została podjęta, podmiot danych ma uprawienie by żądać od administratora ponownego rozpatrzenia sprawy. Administrator ma na to 21 dni[35].

c. Ochrona danych wrażliwych

Rozpatrując temat profilowania, które może prowadzić do dyskryminacji należy podkreślić znaczenie ochrony tzw. danych wrażliwych (szczególnych, sensytywnych). Istnienie informacji którym przysługuje specjalna ochrona jest jedną z podstawowych zasad ochrony danych osobowych. Katalog takich danych wyróżnia się ze względu na dużo większe zagrożenie dla naruszenia prywatności czy intymności niż jest to dostrzegane w przypadku innych danych. Kolejnym argumentem jest minimalizowanie zagrożenia dla podjęcia rozstrzygnięć, które mogą prowadzić do dyskryminacji przy uwzględnieniu tych danych[36].

Zasada ochrony danych wrażliwych pojawiła się już w Konwencji nr 108 Rady Europy dotyczącej ochrony danych osobowych [37]. Dokument ten wskazuje, że do danych o szczególnym statusie należy zaliczyć, dane ujawniające: pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne, oraz danych osobowych dotyczących zdrowia lub życia seksualnego nie można przetwarzać automatycznie (art. 6). Konwencja nr 108 stanowi o

[35] D. Korff, *Study on Implementation of Data Protection Directive*, 2002, s. 113-115, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 (odcz. z dn. 17.07.2015).
[36] J. Barta, *op. cit.*, 549.
[37] Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r., Dz.U. 2003.3.25.

generalnym zakazanie przetwarzania tego typu informacji, chyba, że prawo wewnętrzne przewiduje odpowiednie zabezpieczenia.

Z kolei Wytyczne ONZ dotyczące ochrony danych osobowych [38], w pkt. 5 (zakaz dyskryminacji) wskazują, że nie powinno się gromadzić takich danych, które mogą w konsekwencji prowadzić do niezgodnej z prawem lub nieuzasadnionej dyskryminacji. Wytyczne wskazuję na przykłady takich danych, którymi są: informacje o „pochodzeniu etnicznym i rasowym", „kolorze skóry", „życiu seksualnym", „poglądom politycznym, religijnym, filozoficznym oraz innym" oraz „przynależności do związku zawodowego". Wyjątki od tego zakazu mogą być ustanowione tylko: *„w granicach wyznaczonych przez Międzynarodowe Pakty Praw Człowieka oraz inne instrumenty prawa międzynarodowego dotyczące ochrony praw człowieka i zapobiegania dyskryminacji"*.

Na gruncie dyrektywy 95/46 do katalogu danych wrażliwych zaliczono dane ujawniające: *„pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych"* oraz dane dotyczące zdrowia i życia seksualnego. Polska ustawa w art. 27 poszerzyła ten katalog (który jest katalogiem zamkniętym) o informacje dotyczące „przynależności partyjnej i wyznaniowej", „nałogów" i „kodu genetycznego". Zgodnie z tym przepisem zasadą jest zakaz przetwarzania tego typu informacji. Ustawa zawiera jednak liczne wyjątki, które zostały ujęte w formie zamkniętego katalogu (art. 27 ust. 2), który nie pozwala na jego rozszerzającą wykładnię. Dane wrażliwe można więc przetwarzać m.in. gdy: osoba wyrazi na to pisemną zgodę; pozwala na to przepis ustawy szczególnej (przy jednoczesnym stworzeniu gwarancji ochrony); wymaga tego ochrona żywotnych interesów osoby; jest niezbędne do działania kościołów i związków wyznaniowych, świadczenia usług medycznych czy zadań dotyczących zatrudniania pracowników; prowadzenia badań naukowych; dochodzenia prawa przed sądem. Lista tych wyjątków jest więc długa i pozwalająca na dosyć szerokie korzystanie z danych wrażliwych. Wydaje się, że w stosunku do dyrektywy 95/46, u.o.d.o. wprowadza zbyt szerokie zezwolenie w tym zakresie[39]. Dotyczy to chociażby możliwości przetwarzania danych wrażliwych gdy stanowi tak przepis szczególny innej ustawy (art. 27 ust 2 pkt 2). Dyrektywa 95/46 natomiast

[38] Guidelines for the Regulation of Computerized Personal Data Files Adopted by General Assembly resolution 45/95 of 14 December 1990.
[39] J. Barta, *op. cit.*, s. 138.

ustanawia, że wyjątek może powstać tylko w przypadku istnienia ważnego interesu publicznego (art. 8 ust 4).

Należy zauważyć, że katalog danych wrażliwych nie pokrywa się z czynnikami, z powodu zakazana jest dyskryminacja. Jak to wygląda warto zauważyć na podstawie porównania art. 8 Dyrektywy z art. 21 Karty Praw Podstawowych Unii Europejskiej (KPP) oraz polskiej ustawy o ochronie danych osobowych i tzw. ustawy antydyskryminacyjnej[40].

Tab. 1

Dyrektywa 95/46/WE	Karta Praw Podstawowych Unii Europejskiej
Art. 8 1. Państwa Członkowskie zabraniają przetwarzania danych osobowych ujawniających **pochodzenie rasowe lub etniczne**, **opinie polityczne**, **przekonania religijne** lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego.	Artykuł 21 Niedyskryminacja 1. Zakazana jest wszelka dyskryminacja ze względu na płeć, **rasę**, kolor skóry, **pochodzenie etniczne** lub społeczne, cechy genetyczne, język, **religię** lub światopogląd, **opinie polityczn**e lub wszelkie inne, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną.

Pogrubienia oznaczają kategorie, które występują w obydwu aktach. Podkreślenia natomiast wskazują, że kategorie które częściowo się pokrywają.

Tab. 2

Ustawa o ochronie danych osobowych	Ustawa antydyskryminacyjna
Art. 27. 1. Zabrania się przetwarzania danych ujawniających **pochodzenie rasowe lub etniczne**, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak	Art. 1. Ustawa określa obszary i sposoby przeciwdziałania naruszeniom zasady równego traktowania ze względu na płeć, **rasę**, **pochodzenie etniczne**, narodowość, religię, wyznanie, światopogląd,

[40] Por. R. Gellert, K. de Vries, P.de Hert, S. Gutwirth, *A Comparative Analysis of Anti-Discrimination and Data Protection Legislations*, [w:] B. Custers, T. Calders, B. Schermer, T. Zarsky, *Discrimination and Privacy in the Information Society Data Mining and Profiling in Large Databases*, Springer, 2013, s. 61-90.

również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.	niepełnosprawność, wiek lub orientację seksualną oraz organy właściwe w tym zakresie.

Pogrubienia oznaczają kategorie, które występują w obydwu aktach. Podkreślenia natomiast wskazują, że kategorie które częściowo się pokrywają.

Jak widać w powyższych tabelach w gronie danych wrażliwych nie znajdują się takie informacje jak płeć, kolor skóry, pochodzenie społeczne, język, posiadany majątek, urodzenie, wiek. Natomiast część kategorii takich jak np. orientacja seksualna czy niepełnosprawność, cechy genetyczne może być związana z informacjami występującym w katalogu danych wrażliwych. Zależność tą zauważyła m.in. Agencja Praw Podstawowych Unii Europejskiej (APP) w swojej opinii dotyczącej projektu dyrektywy w sprawie przetwarzania danych PNR[41]. APP uznała, że art. 11 projekt dyrektywy stanowi powtórzenie co do zasady art. 8 dyrektywy 95/46/WE. Tymczasem wg. APP istnieje dużo więcej przesłanek zakazujących dyskryminację (jak np. płeć czy wiek). Zdaniem APP projekt dyrektywy dot. PNR powinien zostać poszerzony o te właśnie kategorie, które wprost wynikają z art. 21 KPP.

d. Reforma ochrony danych

W 2012 roku Komisja Europejska zaproponowała projekt rozporządzenia o ochronie danych osobowych, który gruntownie przebudowuje europejskie prawo w tym obszarze. Ogólne rozporządzenie o ochronie danych (dalej: RODO) osobowych ma obowiązywać bezpośrednio w całej Unii Europejskiej, czyli automatycznie zastąpi istniejące przepisy (w Polsce – ustawę

[41] Opinion of the FRA on the Proposal for a Directive on the use of Passenger Name Record (PNR) data, http://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_EN.pdf (odcz. z dn. 17.07.2015).

o ochronie danych osobowych). Obecnie obowiązujące regulacje unijne powstały w latach 90-tych, gdy niewiele osób korzystało z Internetu a wiele technologii informatycznych było w powijakach. Komisja Europejska wyszła więc z założenia, że istniejące przepisy należy zmodernizować i dostosować do nowych wyzwań. Jednym z nich jest stosowanie na szeroką skalę technik profilowania. Projekt rozporządzania przebył już prac w Parlamencie Europejskim[42]. Obecnie trwają negocjacje tzw. trilogu między Parlamentem, Radą a Komisją. Poniższa analiza uwzględnia postanowienia wynikające z wersji przyjętej już przez eurodeputowanych.

Po raz pierwszy na szczeblu unijnym w projekcie RODO pojawiła się definicja profilowania, która została przytoczona już powyżej. Art. 20 ust. 1 wskazuje na prawo podmiotu danych, do sprzeciwu wobec bycia profilowanym. Przed samym profilowaniem osoba, musi zostać wyraźnie poinformowana o tym uprawnieniu.

RODO pozwala na profilowanie, które prowadzi do środków wywołujących skutki prawne dotyczące podmiotu danych lub ma podobnie istotny wpływ na interesy, prawa lub wolności tego podmiotu danych, tylko w określonych przypadkach. Są nim: zawarcie lub realizacja umowy oraz szczególny przepis prawny pod warunkiem, że wprowadzają one dodatkowe gwarancje dla podmiotu danych; oraz zgoda samego podmiotu (art. 20 ust. 2). Wśród gwarancji o których mowa wcześniej należy wskazać m.in. prawo do otrzymania oceny przez człowieka (decyzja wywołująca poważne skutki prawne i faktycznie nie może być oparty tylko na podstawie automatycznego przetwarzania danych) oraz prawo do wyjaśnienia decyzji podętej przy takiej ocenie.

Projekt rozporządzenia stwarza również ważną gwarancję dotyczącą przeciwdziałania dyskryminacji. Zakazane jest więc profilowanie, które prowadzi do dyskryminacji ze względu na rasę pochodzenie etniczne, poglądy polityczne, religię bądź przekonania, przynależność do związków zawodowych, orientację seksualną bądź tożsamość płciową lub skutkuje środkami mającymi taki efekt (art. 20 ust. 3 zd. 1). Zabronione jest również profilowanie, które opiera

[42] Projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) COM (2012) 11, wersja przyjęta przez Parlament Europejski http://www.europarl.europa.eu/sides/getDoc.do;jsessionid=03B470D165FDB86CDD64F05ED80EEB99.node2?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//pl (odcz. z dn. 17.07.2015)

się tylko na danych wrażliwych (art. 20 ust. 3 zd. 2). Projekt RODO wskazuje, że danymi tymi są dane osobowe ujawniające rasę lub pochodzenie etniczne, poglądy polityczne, religię lub światopogląd, orientację seksualną lub tożsamość płciową, przynależność do związków zawodowych i działalność w nich oraz przetwarzania danych genetycznych lub biometrycznych lub danych dotyczących zdrowia lub seksualności, sankcji administracyjnych, orzeczeń sądowych, popełnionych lub domniemanych przestępstw, wyroków skazujących lub powiązanych środków zabezpieczających (art. 9).

Wśród innych gwarancji, które projekt ten ustanawia w kontekście profilowania znajduje się obowiązek administratora danych do wprowadzenia skutecznej ochrony przed dyskryminacją wynikającą z profilowania (art. 20 ust. 3). Obowiązek ten nie został w żaden sposób doprecyzowany. Jednak gdy operacja na danych wywołuje szczególne ryzyka (m.in. profilowanie, na którym opierają się środki wywołujące skutki prawne dotyczące danej osoby lub mające na nią podobnie istotny wpływ) to administrator powinien przeprowadzić specjalne ocenę skutków takich operacji (art. 33 ust. 1 w zw. z art. 32 ust. 2 pkt c). Wśród czynników, które powinien wziąć pod uwagę jest ocena ryzyka dla praw i wolności podmiotów danych, w tym ryzyka dyskryminacji, jakie pociąga za sobą lub jakie wzmacnia dana operacja (art. 33 ust. 2 pkt. c).

Ograniczenia uprawnień podmiotu danych związane z profilowaniem, mogą zostać wprowadzone tylko na podstawie przepisów prawnych, gdy jest to konieczne i proporcjonalne w demokratycznym społeczeństwie. Wśród wymienionych w motywach projektu uzasadnień dla tego ograniczenia jest np. bezpieczeństwo publiczne, ochrona życia ludzkiego, zapobieganie przestępstwom, ważny interes gospodarczy oraz inne szczególnie i zdefiniowane interesy Unii Europejskiej lub państwa członkowskiego (motyw 59).

Projekt w wersji przyjętej przez Parlament Europejski wprowadza wiele nowych gwarancji dotyczących profilowania, tym szczególny zakaz profilowania dyskryminującego. Na uwagę zasługuje jednak fakt, że katalog zakazanych przyczyn dyskryminacji pokrywa się z katalogiem danych wrażliwych a nie katalogiem ujętym art. 21 KPP dotyczącym zakazu dyskryminacji. Trudno jednoznacznie orzec jakie mogą być bezpośrednie skutki takiej konstrukcji, w razie przyjęcia przepisów w takim brzmieniu. Należy również podkreślić,

szerokie możliwości wprowadzenia ograniczeń uprawnień związanych profilowaniem zwłaszcza w sferze bezpieczeństwa publicznego.

2. Zakaz dyskryminacji

Z art. 32 Konstytucji RP wynika zasada poszanowania równości i zakaz dyskryminacji z jakiejkolwiek przyczyny. Dodatkowo art. 33 Konstytucji RP wskazuje jednoznacznie na równe prawa kobiet i mężczyzn, w tym do zabezpieczania społecznego. Zasada równości i niedyskryminacji jest też nieodłączonym elementem międzynarodowego systemu ochrony praw człowieka obecnym m.in. w Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności czy Karcie Praw Podstawowych Unii Europejskiej. Trybunał Konstytucyjny wielokrotnie podkreślał, że z zasady równości, wynika nakaz jednakowego traktowania podmiotów prawa w obrębie określonej klasy (kategorii). Wszystkie podmioty prawa charakteryzujące się w równym stopniu daną cechą istotną (relewantną), powinny być traktowane równo, a więc według jednakowej miary, bez zróżnicowań, zarówno dyskryminujących, jak i faworyzujących[43]. Ponadto Trybunał Konstytucyjny wskazał, że „*jeżeli prawodawca różnicuje podmioty prawa, które charakteryzują się wspólną cechą istotną, to wprowadza on odstępstwo od zasady równości. Jest ono dopuszczalne, jeżeli zostały spełnione trzy warunki: po pierwsze, wprowadzone przez prawodawcę różnicowania muszą być racjonalnie uzasadnione (muszą mieć związek z celem i treścią przepisów, w których zawarta jest kontrolowana norma); po drugie, waga interesu, któremu ma służyć różnicowanie podmiotów podobnych, musi pozostawać w odpowiedniej proporcji do wagi interesów, które zostaną naruszone w wyniku różnego traktowania podmiotów podobnych; po trzecie, różnicowanie podmiotów podobnych musi znajdować podstawę w wartościach, zasadach lub normach konstytucyjnych*”[44] .

Na gruncie ustawowym do przeciwdziałania dyskryminacji kluczowe znaczenia mają przepisy o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania (tzw. ustawa antydyskryminacyjna)[45]. Akt ten określa obszary i sposób

[43] Por. Wyrok Trybunału Konstytucyjnego z dnia 23 października 2001 r., sygn. K. 22/01
[44] Wyrok Trybunału Konstytucyjnego z dnia 19 lutego 2001 r., sygn. SK 14/00.
[45] Ustawa z dnia 3 grudnia 2010 r. o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania, Dz.U.2010.254.1700.

przeciwdziałania naruszaniu zasady równego traktowania. Zakazuje nierównego traktowania ze względu na płeć, rasę, pochodzenie etniczne, narodowość, religię, wyznanie, światopogląd, niepełnosprawność, wiek lub orientację seksualną (art. 8 ust. 1 pkt. 4). Za nierówne traktowania ustawa ta rozumie m.in. dyskryminacją bezpośrednią i dyskryminacją pośrednią. Obszarami objętymi ustawą są m.in. kształcenie zawodowe, oświata, opieka zdrowotna, zabezpieczanie społeczne, sfera zawodowa, prowadzenie działalności gospodarczej oraz usług. Wyłączone są natomiast: swoboda wybory strony umowy (w ograniczonym zakresie), życie prywatne, działalność kościołów i związków wyznaniowych czy warunków wjazdu i wyjazdu z terytorium RP. Należy jednak zaznaczyć, że ustawa antydyskryminacyjna wprowadza różne kryteria zakazu nierównego traktowania w poszczególnych obszarach. Np. w przypadku dostępu do zabezpieczenia społecznego zakazane nierównie traktowanie z powodu płci, rasy, pochodzenia etniczne lub narodowości, ale już nie zw. na niepełnosprawności czy orientację seksualną.

Ustawa wskazuje również na środki prawne dla ochrony przed naruszeniem zasady równego traktowania. Każdy wobec kogo ją naruszono, może ubiegać się o odszkodowanie (art. 13 ust. 1). W postpowaniu tym stosuje się zasady postępowania cywilnego. Ustawa stosuje zasadę odwróconego ciężaru dowodu (art. 13 ust. 2). Osoba, która twierdzi, że naruszono zasadę równego traktowania powinna uprawdopodobnić ten fakt. Jednak ciężar dowodu spoczywa na osobie, której zarzut jest czyniony (art. 14 ust. 2-3).

Przepisy bezpośrednio dotyczące zakazu dyskryminacji znajduję się również m.in. w Kodeksie pracy[46]. Zgodnie z jego postanowieniami (rozdział IIa), niedopuszczalna jest dyskryminacji w zatrudnieniu w szczególności ze względu na: płeć, wiek, niepełnosprawność, rasę, religię, narodowość, przekonania polityczne, przynależność związkową, pochodzenie etniczne, wyznanie, orientacje seksualną, a także ze względu na zatrudnienie na czas określony lub nieokreślony albo w pełnym lub niepełnym wymiarze czasu pracy.

3. Przykłady szczególnego uregulowania profilowania:

a. PNR

[46] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy, Dz.U. 1974 nr 24 poz. 141 ze zm.

W 2011 roku Komisja Europejska przedstawiła projekt dyrektywy w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania (tzw. dyrektywa PNR) [47] . Akt ten ma umożliwić tworzenie systemów informatycznych pozwalających na analizowanie danych o pasażerach linii lotniczych (PNR)[48] na potrzeby ochrony porządku publicznego – zwalczania terroryzmu czy innych poważnych przestępstw. Projekt ten wzbudza wiele emocji z różnych względów. Jednym z nich jest umożliwienie masowego przetwarzania danych o wszystkich pasażerach lotów lecących do i z terenu Unii Europejskiej, co może naruszać zasadę proporcjonalności w naruszaniu praw podstawowych np. prawa do ochrony danych osobowych.

W uzasadnieniu projektu Komisja Europejska wskazuje, że dane PNR mogą być wykorzystywane przez organy ścigania na trzy sposoby: reaktywnie (np. w postępowaniu przygotowawczym i sądowym, po ujawnieniu przestępstwa); w czasie rzeczywistym (przed przybyciem lub odlotem pasażerów w celu zapobieżenia przestępstwom, obserwacji lub zatrzymania osób zanim przestępstwo zostanie popełnione, lub ponieważ zostało już popełnione albo jest właśnie popełniane) oraz aktywnie (do analizy i tworzenia kryteriów oceny, które mogś później wykorzystywane do oceny pasażerów przed przybyciem i odlotem). Kryteriami które mogą być brane do takiej analizy są trasy lotów czy zachowania pasażerów. Wykorzystywanie danych PNR ze swojej istoty związane jest więc z tworzeniem

[47] Projekt Dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania, COM (2011) 32.

[48] Wśród danych PNR znajdują się takie informacje jak: Kod identyfikacyjny danych PNR,Data rezerwacji/wystawienia biletu, Data(-y) planowanej podróży, Imię i nazwisko, Adres i dane kontaktowe (numer telefonu, adres e-mail), Wszystkie informacje dotyczące formy płatności, w tym adres na fakturze, Kompletna trasa podróży dla określonych PNR, Informacje dotyczące programów lojalnościowych, Biuro podróży/ agencja turystyczna, Dane o statusie podróży pasażera, w tym potwierdzenia, stan odprawy biletowo-bagażowej, dane typu: pasażer nie stawił się lub pasażer nabył bilet w czasie odprawy, bez wcześniejszej rezerwacji, Informacje o rozdzieleniu danych PNR, Uwagi ogólne (w tym wszelkie dostępne informacje o małoletnich bez opieki w wieku poniżej 18 lat, takie jak imię i nazwisko, płeć, wiek, języki, którymi włada, imię i nazwisko oraz dane kontaktowe opiekuna w momencie odlotu oraz rodzaj więzi łączącej go z małoletnim, imię i nazwisko opiekuna w momencie lądowania oraz rodzaj więzi łączącej go z małoletnim, przedstawiciel obecny przy odlocie i przylocie), Informacje o wystawieniu biletu, w tym numer biletu, data wystawienia biletu i bilety w jedną stronę, informacja o automatycznie skalkulowanej taryfie, Numer miejsca na pokładzie i inne informacje o miejscu, Informacje o wspólnym kodzie, Wszystkie informacje o bagażu, Liczba oraz imiona i nazwiska innych podróżnych wymienionych w PNR, Wszelkie zgromadzone dane pasażera przekazywane przed podróżą (API), Wszystkie dotychczasowe zmiany danych PNR wymienionych w pkt 1–18.

pewnym modeli (profili) i szacowaniu na ich podstawie ryzyka, jakie powoduje konkrenta jednostka.

Sam projekt dyrektywy jasno stwierdza, że określone organy nie mogą podjąć żadnych decyzji mających negatywne skutkie prawne lub w inny poważny sposób wpływają na sytuację jednostki tylko na podstawie automatcznego przetwrzania danych PNR (art. 5 ust. 6). W projcie wskazuje się również, że ocena pasażerów na podstawie danych PNR odbywa się w celu identyfikacji osób, które mogą być zamieszane w przestępstwo terrorystyczne lub poważne przestępstwo. Co jednak istotne wszelkie przypadki skojarzenia danych, które wyniakją z analizy automatycznej, muszą być rozstrzygnięcie indywidualnie przecz człowieka (art. 4 ust. 2 pkt a).

Inną zastosowaną gwarancją w projkecie jest zakaz przetwarzania danych ujawniających na pochodzenie rasowe lub etniczne, wierzenia religijne lub filozoficzne, poglądy polityczne, przynależność do związków zawodowych albo zdrowie lub życie seksualne. Jeżeli jednostki odpowiedzialne za analizę danych PNR uzyskają takie informacje muszą je niezwłocznie usunąc. Dodatkowo projekt zakazuje podejmowania decyzji wynikających z analizy danych PNR, ze względu kryteria tożsame z katalogiem danych, których przetwarzanie jest zakazane. Z kolei art. 4 ust 3 wskazuje, że ocena pasażerów przed ich przylotem czy odlotem dokonuje się w sposób niedyskryminacyjny.

Jak widać w projekcie dyrektywy PNR zminimalizowano wystąpienie ryzyka dyskryminacji bezpośredniej i dyskryminującego profilowania. Należy jednak zaznaczyć, że zakres danych, których przetwarzanie jest zakazane jest tożsamy z katalogiem danych wrażliwych ujętych w dyrektywie 95/46/WE, nie zaś np. zaś z katalogiem ujętym w art. 21 Karty Praw Podstawowych. Problem ten dostrzegała Agencja Praw Podstawowych (patrz wyżej). Co więcej bardzo ogólna kategoria danych PNR, może ujawniać dane wrażlie np. dotyczące wyznania czy narodowości na podstawie serwowanego w trakcie lotu posiłku. APP podniosła również problem dyskryminacji pośredniej, która może wynikać ze stosowania analizy danych PNR. Osoba może np. być przedmiotem działaniania organów ścigania tylko przez brzmienie swojego naziwska czy trasę wybieranego lotu. APP by przeciwdziałać takiemu podejściu rekomendowała gromadzenie danych statystycznych na podstawie danych PNR, które pozwoliłby wykrywanie praktyk dyskryminacyjnych. Takie dane oczywiście powinny

być w pełni zanonimizowane i nie pozwalające na identyfikację. Dodatkowo APP podkreśliła, że w wytycznych dotyczących przeglądu funkcjonowania dyrektywy PNR, należy uzpełnić o obowiązek badania czy realizowana jest zasady niedyskryminacji.

b. Profilowanie pomocy dla bezrobotnych

W maju 2014 roku w życie weszła nowelizacja ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw[49] oraz rozporządzenie Ministra Pracy i Polityki Społecznej w sprawie profilowania pomocy dla bezrobotnego[50]. Na podstawie ww. aktów prawnych wprowadzono mechanizm profilowania pomocy dla osób bezrobotnych. U podstaw wprowadzenia tego mechanizmu legły argumenty dotyczące zwiększenia indywidualnego podejścia w miejscach pracy, zwiększenia efektywności urzędów pracy oraz lepszego zarządzania środkami publicznymi.

Znowelizowana ustawa poszerzyła zakres obowiązków samorządów powiatu w zakresie polityki rynku pracy o ustalanie profili pomocy dla bezrobotnych (art. 9 ust. 1 pkt 4a). Ustawa definiuje profil pomocy jako „zakres form pomocy określonych w ustawie". Ustawa określa podział na trzy profile pomocy, nie określa jednak ich charakterystyki. Wskazuje tylko jakie formy pomocy są adresowane do każdego z wymienionych profili. W przepisach określono zakres pomocy adresowanych do konkretnych profili (art. 33 ust 2c). Należy nadmienić, że zakres oferowanych form pomocy jest bardzo różny i jest on skonstruowany w taki sposób, że określone profili (I i II) nie mogą uzyskać niektórych form.

Z kolei według par. 2 rozporządzenia dot. profilowania pomocy dla bezrobotnego ustalenie profilu odbywa się poprzez analizę sytuacji bezrobotnego i jego szans na rynku pracy. Dwiema zmiennymi, branymi pod uwagę jest "oddalenie od rynku pracy" oraz "gotowość do wejścia lub powrotu na rynek pracy". W trakcie analizy bierze się pod uwagę takie dane jak: wiek, płeć, poziom wykształcenia, umiejętności, uprawnienia i doświadczenie zawodowe, stopień niepełnosprawności określony posiadanym orzeczeniem o niepełnosprawności, czas pozostawania bez pracy, miejsce zamieszkania pod względem oddalenia od potencjalnych

[49] Ustawa z dnia 14 marca 2014 r. o zmianie ustawy o promocji zatrudnienia i instytucjach rynku pracy oraz niektórych innych ustaw, Dz.U.2014.598.
[50] Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 14 maja 2014 r. w sprawie profilowania pomocy dla bezrobotnego, Dz.U.2014.631.

miejsc pracy i dostępność do nowoczesnych form komunikowania się z powiatowym urzędem pracy i pracodawcami, zaangażowanie w samodzielne poszukiwanie pracy, gotowość do dostosowania się do wymagań rynku pracy, dyspozycyjność, powody skłaniające do podjęcia pracy, powody rejestracji w powiatowym urzędzie pracy, dotychczasową oraz aktualną gotowość do współpracy z powiatowym urzędem pracy, innymi instytucjami rynku pracy lub pracodawcami.

Dane, które podlegają analizie w trakcie ustalenia profilu pochodzą z dwóch źródeł. Z jednej strony przetwarza się informacje, które są przetwarzana przy okazji rejestracji w urzędzie pracy na tzw. „karcie rejestracyjnej". Z drugiej zaś pracownicy przeprowadzają specjalny ustrukturyzowany wywiad. Samo ustalenie profilu odbywa się za pomocą systemu informatycznego, który udostępnia minister pracy.

Rozporządzanie wskazuje, że urząd może ponownie ustanowić profil pomocy, jeżeli w trakcie trwania tzw. indywidualnego plany działania nastąpi zmiana w sytuacji bezrobotnego (dotycząca danych wskazanych w rozporządzeniu). Profil pomocy jest ponownie ustalany, gdy w określonych w rozporządzeniu okresach, nie udało się przywrócić bezrobotnego na rynek pracy. Nie wspomina się jednak w żaden sposób czy bezrobotny może wyrazić sprzeciw wobec ustalonego profilu pomocy lub zawnioskować o jego zmianę.

W trakcie profilowania urząd pracy nie przetwarza wielu danych wrażliwych, w zasadzie jest nimi niepełnosprawność oraz informacje dotyczące ograniczeń zdrowotnych, wpływających na potencjał zatrudnienia bezrobotnego. Dodatkowo o przydzielaniu do określonego profilu decydują takie cechy jak: wiek czy płeć. W praktyce może więc dochodzić do różnicowania sytuacji konkretnej osoby bezrobotnej ze względu na wymienione powyżej kryteria, co można uznać za stosowanie zakazanych praktyk dyskryminacyjnych.

Przydzielanie do konkretnego profilu może w ogóle zablokować dostęp do jakichkolwiek form wsparcia. Analiza przepisów ustawy wskazuje, że w wielu przypadkach organizowanie przez powiatowe urzędy pracy oraz jednostki samorządu terytorialnego konkretnych form wsparcia ma charakter fakultatywny (np. Program Aktywizacja i Integracja, art. 62a ustawy o promocji zatrudnienia). W praktyce jest ono uzależnione od środków finansowych i organizacyjnych, jakimi dysponują te podmioty. Problem ten dotyczy w szczególności form

wsparcia proponowanych dla III profilu pomocy. W konsekwencji osoby zakwalifikowane do tego profilu mogą nie uzyskać żadnej pomocy ze strony powiatowego urzędy pracy.

Przepisy dotyczące profilowania pomocy dla osób bezrobotnych nie zawierają żadnych gwarancji dotyczących przeciwdziałania dyskryminacji. Z kolei kwestie dotyczące przetwarzania danych i automatycznego podejmowania decyzji zostały uregulowane bardzo efemerycznie. Nie zastosowano np. możliwości odwołania się od profilu, zakazu oparcia decyzji tylko o automatyczne przetwarzanie danych czy wskazane powyżej „prawa do bycia wysłuchanym".

Część III
STOSOWANIE PRAWA I DEBATA PUBLICZNA

1. Przykłady orzecznictwa

W kontekście profilowania warto przywołać wyrok Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w sprawie Association Belge des Consommateurs Test-Achats ASBL i inni przeciwko Belgii[51]. Trybunał w tej sprawie rozpatrywał czy płeć może być brana pod uwagę jako czynnik wpływający na ustalenie składki ubezpieczeniowej. W sprawie tej stwierdzono, że umożliwienie państwom członkowskim uchylenia się od zasady równości płci, bez żadnych ograniczeń czasowych jest działaniem sprzecznym z zasadą równego traktowaniu kobiet i mężczyzn w odniesieniu do kalkulacji składek i świadczeń ubezpieczeniowych. Trybunał uznał również, że *„w celu zapewnienia równego traktowania kobiet i mężczyzn stosowanie płci jako czynnika aktuarialnego nie powinno powodować dla ubezpieczonych różnic w odniesieniu do składek i świadczeń"*. W orzeczeniu tym powołano się właściwie tylko na przepisy dotyczące zakazu dyskryminacji, co było spowodowane tym, że podmiotom inicjującym postępowanie była organizacja konsumencka, a nie osoba fizyczna, która może wywodzić swoje uprawnienia z prawa ochrony danych osobowych. Można tylko domniemać czy w podobnej sytuacji przepisy dotyczące ochrony danych mogą wzmocnić zakres ochrony jednostki. Problemem w tym kontekście może być charakter samego profilowania. W przypadku Test-Achats doszło do pewnego profilowania grupowego

[51] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 1 marca 2011 r., sygn. C-236/09.

i nie jest oczywiste, czy dochodzi do przetwarzania danych osobowych. Grupa Robocza Art. 29 w swojej opinii doradczej wskazuje, jednak, że *„Również element <<cel>> może sprawiać, że informacja <<dotyczy>> danej osoby. Można uznać, że element <<cel>> występuje, jeżeli dane są lub mogą być wykorzystywane, biorąc pod uwagę wszystkie okoliczności danej sprawy, w celu oceny osoby, jej traktowania w określony sposób lub też wpływania na jej status lub zachowanie”*[52].

Z kolei w sprawie dotyczącej wysokości składki emerytalnej, rzecznik generalny TSUE – zwracając uwagę na relacje między wykorzystaniem danych statystycznych a dyskryminacją – zauważył, że *„można by wyobrazić sobie sytuację (która jest jak najbardziej prawdopodobna), w której dane statystyczne pokazują, iż członkowie jednej grupy etnicznej żyją średnio dłużej niż członkowie innej grupy etnicznej. Uwzględnianie tych różnic przy określaniu korelacji pomiędzy wkładami a uprawnieniami w ramach wspólnotowego systemu emerytalnego byłoby całkowicie niedopuszczalne”*[53] .

Na gruncie krajowym ważne znaczenie ma orzeczenie niemieckiego Federalnego Trybunały Konstytucyjnego z roku 2006 roku w sprawie, która dotyczyła specjalnego programu gromadzenia danych na potrzeby zapobiegania przestępstw pod nazwą Rasterfahndung[54]. Program ten umożliwiał na „wyłapywanie” członków organizacji terrorystycznych, poprzez analizę danych pochodzących z publicznych i prywatnych baz danych. Na podstawie tych informacji tworzono profile osób, które miały potencjalnie stanowić ryzyko. Wśród czynników ryzyka wyróżniono: bycie mężczyzną, Muzułmaninem, pochodzenie z jednego z 26 krajów (głównie muzułmańskich). Zdaniem sądu konstytucyjnego gromadzenie i analizowanie danych, jest dopuszczalne wówczas gdy istnieje zidentyfikowane zagrożenie dla bezpieczeństwa publicznego. Sama przesłanka bezpieczeństwa publicznego – rozumiana abstrakcyjnie – nie może stanowić podstawy dla naruszenia autonomii informacyjnej. Dodatkowo sąd uznał, że zastosowana metoda analizy danych może mieć stygmatyzujący efekt oraz prowadzić do dyskryminacji w życiu codziennym.

---

[52] Grupa Robocza Art. 29, Opinia 4/2007 w sprawie pojęcia danych osobowych przyjęta w dniu 20 czerwca, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf (odcz. z dn. 17.07.2015)

[53] Opinia Rzecznika Generalnego F. G. Jacobsa przedstawiona w dniu 27 października 2005 r. w sprawie C-227/04 P.

[54] Wyrok Federalnego Trybunału Konstytucyjnego z dnia 4 kwietnia 2006 r, syg. 1 BvR 518/02 - https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2006/04/rs20060404_1bvr051802.html (odcz. z dn. 17.07.2015)

W sprawach rozpatrywanych przez polskie sądy profilowania lub automatyczne metody podejmowania decyzji zdarzają się niezwykle rzadko. Jednym z wyjątków jest temat scoringu kredytowego. Wojewódzki Sąd Administracyjny w Warszawie uznał w orzeczeniu z 24 listopada 2005 roku[55], że decyzja o odmowie pożyczki w związku z negatywną oceną scoringową jest podejmowana automatycznie przez system informatyczny i w związku z tym narusza zakaz ujęty w art. 26a ust 1 u.o.d.o. Wyrok sądu był efektem zaskarżenia wcześniejszej decyzji GIODO. Zdaniem sądu decyzja o odmowie udzielania pożyczki była podjęta na podstawie scoringu, który jest wynikiem operacji na danych prowadzonym s systemie informacyjnym. Program, który posiadał podmiot prowadzący scoring pozwalał na zestawienie zadanych cech statystycznych, demograficznych w jeden wynik w postaci punktacyjnej. Sąd uznał, że w tym przypadku decyzja odmowna była podjęta automatycznie, w związku z czym jest niezgodna z art. 26a ust 1 u.o.d.o.

2. Rekomendacje organów międzynarodowych i europejskich

a. Rada Europy

Profilowanie jest przedmiotem rekomendacja Komitetu Ministrów państw członkowskich Rady Europy z 2010 roku[56]. We wstępie do rekomendacji komitet wskazuje, że tworzenie profili może prowadzić do naruszenia prawa do prywatności, danych osobowych oraz zasady niedyskryminacji (m.in. poprzez nieusprawiedliwione pozbawienie dostępu do pewnych dóbr czy usług). Podkreśla również, że ryzyko dyskryminacji może szczególnie wystąpić gdy przy profilowaniu stosowane są dane szczególnie chronione. Same rekomendacje jasno wskazują, że przy tworzeniu profili powinny obowiązywać ogólne zasady przetwarzania danych oraz uprawnienia osób, których dane dotyczą. W kilku miejscach rekomendacja zwraca uwagę na problemy, które w sposób szczególny dotyczą profilowania. Jest nim np. kwestia jakości danych. Zgodne z pkt. 3.9 rekomendacji, administrator powinien podejmować działania, które minimalizowałyby niedokładność danych i ograniczyło ryzyko błędów „nierozerwalnie związane z profilowaniem". Innym obowiązkiem powinna być okresowy przegląd jakości

[55] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawiez dnia 24 listopada 2005 r. II SA/Wa 1335/05.
[56] Rekomendacja Komitetu Ministrów państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profilii, CM/Rec (2010) 13, polskie tłumaczenie http://www.giodo.gov.pl/plik/id_p/2155/j/pl/. (odcz. z dn. 17.07.2015).

wykorzystywanych danych oraz wniosków statystycznych (pkt 3.10). Komitet postuluje również, żeby gromadzenie i przetwarzanie danych wrażliwych na potrzeby profilowania, było zakazane, za wyjątkiem sytuacji gdy jest to niezbędne i jeżeli istnieją odpowiednie zabezpieczenia (pkt 3.11). Osobom powinny również przysługiwać odpowiednie uprawnienia. Jednym z nich jest prawo do informacji o: wykorzystywaniu danych do tworzenia profili, celu profilowania, wykorzystywanych kategoriach danych, długości przechowywania danych, przewidywanych efektów przypisania profilu (pkt 4.1). Osoba powinna mieć również prawo do wyrażenia sprzeciwu wobec decyzje mające skutki prawne lub wpływające na jej sytuacji, jeżeli została ona podjęta wyłącznie na podstawie profilowania. Wyjątkiem są tutaj jednak podstawy prawne lub wykonanie umowy (pkt 5.5).

b. Grupa Robocza art. 29

Stanowisko dotyczące uregulowania profilowania wyraziła również Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych tzw. Grupa Robocza Art. 29[57]. Zdaniem przepisy powinny regulować nie tylko decyzje oparte na profilowaniu (jak ma to miejsce m.in. w dyrektywie 95/46/WE), ale również sam proces gromadzenia danych na potrzeby profilowania i tworzenia profili. Wynika to m.in. często z tego, że profilowanie często odbywa się poza wiedzą osób, których ono dotyczy. Grupa postuluje również by zwiększyć uprawnienia informacyjne podmiotu danych w zakresie uzyskiwania informacji o danych wykorzystywanych w trakcie profilowania, celu profilowania oraz logiki dotyczące automatycznego przetwarzania danych. Osoby powinny mieć również uprawnienie do dostępu, zmiany lub usunięcia profilu, który jest im przypisany. Innym uprawnieniem powinna być możliwość wyrażenia sprzeciwu wobec decyzji, która jest podjęta na podstawie profilu lub podjęcia tej decyzji przy udziale człowieka.

c. Parlament Europejskich

Parlament Europejski w 2010 roku podjął rezolucję dotyczące tworzenia profili w oparciu na

[57] Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, Adopted on 13 May 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf (odcz. z dn. 17.07.2015).

pochodzenie rasowe i etniczne na potrzeby walki z terroryzmem i przeciwdziałania przestępczości[58]. Parlament podkreślił w niej m.in. samo profilowanie jest przykładem gdzie odchodzi się od ogólnej zasady, zgodnie z którą decyzje organów śledczych powinny się opierać na zachowaniu danej osoby. Dodatkowo podkreślił, że „tworzenie profili zaciera granice między dopuszczalną obserwacją i problematyczną inwigilacją na masową skalę, przy której dane gromadzi się dlatego, że są przydatne, a nie w określonych celach, co może prowadzić do bezprawnej ingerencji w życie prywatne". Samo zaś tworzenie profili w oparciu o pochodzenie etniczne może nasilić wrogość i ksenofobię wśród społeczeństwa w odniesieniu do osób o konkretnym pochodzeniu etnicznym, narodowym czy wyznaniu oraz prowadzić do dyskryminacji. Parlament rekomendował by przetwarzanie danych osobowych do celów walki z przestępczością i terroryzmem opierało się na jasnych i szczegółowych przepisach prawnych. Jednoczenie zakazane powinno być masowe przechowywanie danych, a wszelkie naruszenia przepisów surowo karane. Parlament wskazuje na potrzebę zdefiniowania tworzenia profili oraz zakaz gromadzenia danych wyłącznie na podstawie szczególnego pochodzenia rasowego lub etnicznego, przekonań religijnych, orientacji seksualnej czy zachowania, opinii politycznych lub członkostwu w specyficznych ruchach czy organizacjach. Sam sporządzanie profili w stosunku do osób niepodejrzewanych o konkretne przestępstwo ma być uzależnione od spełniania surowych wymóg konieczności i proporcjonalności. Dostęp do profili i danych gromadzonych przez służby i policję powinien podlegać zawsze kontroli sądowej. Niezbędne jest również ustanowenie gwarancji i procedur odwoławczych w przypadku tworzenia profili prowadzących do dyskryminacji. Parlament wskazuje również, że niezbędne jest gromadzenie statystyk dotyczących działań organów egzekwowania prawa, które w sposób nieproporcjonalny skupiają się na mniejszościach etnicznych. Gromadzenie takich danych powinno spełniać wysokie kryteria ochrony danych osobowych.

Część IV

[58] Zalecenie Parlamentu Europejskiego z dnia 24 kwietnia 2009 r. dla Rady wraz z projektem zalecenia Parlamentu Europejskiego dla Rady w sprawie problemu tworzenia profili - zwłaszcza w oparciu o pochodzenie etniczne i rasę - w dziedzinie walki z terroryzmem, egzekwowania prawa, imigracji, ceł i kontroli granicznej, 2008/2020(INI), Dz.U.UE C z dnia 8 lipca 2010 r.

PODSUMOWANIE I REKOMENDACJE

Jak wskazałem powyżej profilowanie jako metoda kategoryzowania osób i podejmowania na tej podstawie decyzji, niesie za sobą wiele zagrożeń. Obecne przepisy prawne – zarówno te krajowe jak i europejskie – nie stwarzają jednak odpowiednich gwarancji dla ochrony praw i wolności człowieka w tym kontekście. Profilowanie w związku, z tym, że staje się metodą niezwykle popularną, wkraczającą w różne dziedziny funkcjonowania państwa, społeczeństwa i gospodarki wymaga dobrych i jasnych reguł, które mogłyby te zagrożenie minimalizować.

Kluczowe oczywiście są ogólne regulacje dotyczące zarówno zasad ochrony danych osobowych jak i przeciwdziałania dyskryminacji. Profilowanie nierozłącznie wiąże się z przetwarzaniem danych. Obecnie obowiązujące europejskie przepisy w tym zakresie nie są dostosowane do wymogów świata, w którym technologie zaczynają dogrywać coraz ważniejszą rolę. Potrzebne są m.in. doprecyzowanie samej definicji danych osobowych, silne gwarancje dotyczące wyraźnej zgody na przetwarzania danych, zwiększenie transparentności samego procesu i ograniczenie możliwości przekazywania danych do krajów, które nie oferują adekwatnych standardów. Te zmiany być może wprowadzi reforma ochrony danych osobowych. Z kolei przepisy antydyskryminacyjne często mają tylko fragmentaryczny charakter i ograniczony zakres (np. dotyczący zatrudnienia czy wybranych usług). W polskim systemie też brakuje silnego organu, którego praca skupiałaby się na problemie nierównego traktowania. Jednak bez względu na te ogólne problemy dotyczące obydwu obszarów prawa, chciałbym poniżej wskazać kluczowe – moim zdaniem – postulaty zmian przepisów prawnych lub ich stosowania, dotyczących same już profilowania.

I. Ogólny zakaz profilowania

Ogólne przepisy prawne powinny wprowadzić generalny zakaz stosowania technik opartych na profilowaniu, bez względu na to czy prowadzi ono do podjęcia decyzji prawnych lub innych mających wpływ na sytuację danej osoby. Od zakazu mogą istnieć wyjątki wynikające z zawarcia czy wykonywania umowy lub jednoznacznych i precyzyjnych przepisów prawnych umieszczonych w ustawie. Jednak takie wyjątki powinny mieć zastosowanie tylko

wtedy gdy sam profilowanie jest konieczne i niezbędne oraz przy wprowadzeniu odpowiednich gwarancji ochrony (o których poniżej).

II. Zwiększenie przejrzystości

Bardzo często algorytmy stosowane przy profilowaniu objęte są tajemnicą handlową. W przypadku profilowania przez władze publiczne metodologia tworzenia kategorii również bywa objęta tajemnicą. Wydaje się więc, że przepisy prawne powinny w sposób jednoznaczny wskazywać, że osoba ma prawo do zapoznania się z kryteriami na podstawie, których utworzono przypisany do niej profil. Uprawienie takie nie powinno tylko obejmować informacji o wykorzystywanych danych, ale również metod ich przetwarzania, wyciąganych wnioskach czy przypisywanej punktacji. Osoby muszą również wiedzieć, że w ogóle zostały sprofilowanie, jakie konsekwencje z tego wynikają oraz komu informacje o profilu mogą zostać przekazane. Moim zdaniem informacje takie powinny być obowiązkowo przedstawiane każdej osobie, zanim w ogóle dojdzie do tworzenia profilu. Zapewnienie przejrzystości ma również zagwarantować, że decyzje podjęte na podstawie profilowania nie będą prowadzić do dyskryminacji.

III. Gwarancje proceduralne

Gdy profilowanie prowadzi do podjęcie określonych rozstrzygnięć wobec konkretnej osoby, powinna ona mieć zawsze możliwość odwołania się od niej. Uprawienie takie powinno być realizowane w taki sposób, że sprawa jest ponownie rozpatrywana i rewidowana przez człowieka a nie algorytm. Jeżeli osoba wciąż nie zgadza się z takim rozstrzygnięciem, musi istnieć możliwość zwrócenia się do niezależnego organu czy sądu, który będzie rozpatrywał sprawę. Przed ostatecznym podjęciem decyzji opartej na profilowaniu, osoba powinna mieć możliwość wyrażenia swojego zdania na temat rozstrzygnięcia. Powinno ona znajdować się w dokumentacji dotyczącej konkretnej sprawy i w uzasadnionych sytuacjach prowadzić do zmiany podjętej decyzji.

IV. Dane wrażliwe

Uważam, że należy rozważyć możliwość ujednolicenia katalogu danych wrażliwych i zakresu przyczyn, dla których zakazana jest dyskryminacja. W przypadku gdy przepisy ochrony danych osobowych regulują również konsekwencje profilowania, powinny odwoływać się nie tylko do postanowień dotyczących katalogu danych szczególnie chronionych, ale również ustawodawstwa antydyskryminacyjnego. Uważam również, że przepisy powinny wskazywać na zakaz profilowania, które opiera się o katalog danych wrażliwych lub takie cechy jak płeć czy wiek.

V. Ocena wpływu na prawa człowieka

Podmioty przed wdrażaniem technik opartych na profilowaniu powinny mieć obowiązek przeprowadzenia szczegółowej oceny tych technik ze względu na prawa i wolności człowieka. Ocena taka powinna szczególnie obejmować wpływ na ochronę danych osobowych oraz zasadę równego traktowania i być przeprowadzona w formie pisemnej, dostępna dla odpowiednich organów kontrolnych. W przypadku instytucji publicznych stosujących profilowanie, powinny one mieć obowiązek przeprowadzania cyklicznej ewaluacji stosowanych metod profilowania pod kątem ich skuteczności, niezbędności oraz wpływu na prawa podstawowe.

VI. Gwarancje w aktach szczególnych

Gwarancje dotyczące profilowania – jak transparentność, możliwość odwołania się czy zakaz przetwarzania danych wrażliwych powinny być zawsze zwarte w przepisach prawnych, które regulują szczególne przypadki profilowania (tj. dyrektywa PNR). Powtórzenie takie wydaje mi się niezbędne dla zapewnienia jasności przepisów i wzmocnienia ochrony praw jednostki. Jest to szczególnie istotne w przypadkach, gdy profilowanie stosowane jest przez organy ścigania.

VII. Regulacja i kontrola

Profilowanie i jego konsekwencje powinny podlegać szczególnej kontroli ze strony niezależnych organów, zajmujących się ochroną danych osobowych, ochroną konsumentów i

zakazem dyskryminacji. Organy takie powinny mieć bezwzględna możliwość skontrolowania stosowanych metod przetwarzania danych (w tym algorytmów), która nie byłaby ograniczana np. tajemnicą handlową. Warto rozpatrzyć postulat by podmioty, które decydują się na korzystanie z metod profilowania, musiały uprzednio uzyskiwać na to zgodę odpowiedniego organu. Postulat taki mógłby mieć zastosowanie w tak szczególnych obszarach jak zatrudnienie, ochrona zdrowia, przeciwdziałanie przestępczości czy bankowość. Organy kontroli mogłyby przed wydaniem zgody, badać reguły profilowania pod kątem ich zgodności z zasadami ochrony danych osobowych, równego traktowania czy ochrony konsumentów.

VIII. Sprawozdawczość

By ograniczyć możliwość występowania dyskryminacji pośredniej, w przypadku stosowania decyzji opartych na profilowaniu powinna być prowadzona szczegółowa statystyka. Mogłaby ona obejmować informacje o tym jakie decyzje zostały podjęte, wobec jakich grup, jakie czynniki zostały brane pod uwagę. Postulat ten powinien mieć szczególne zastosowanie w przypadku korzystania z profilowania przez policję czy służby. Gromadzenie tych danych powinno być zgodne z zasadami ochrony danych osobowych i w pełni anonimowe.